美亚柏科 中锐电子◎资助出版

侦查中电子数据取证

Electronic Data Collection in Investigation

李双其 林伟 著

申强 审定

知识产权出版社

国百佳图书出版单位

美亚柏科 中锐电子◎资助出版

侦查中电子数据取证

Electronic Data Collection in Investigation

李双其 林伟 著

申强 审定

知识产权出版社

全国百佳图书出版单位

图书在版编目（CIP）数据

侦查中电子数据取证/李双其，林伟著．--北京：知识产权出版社，2018.6

ISBN 978-7-5130-5580-2

Ⅰ.①侦… Ⅱ.①李… ②林… Ⅲ.①计算机犯罪—证据—数据收集—研究—中国 Ⅳ.①D924.364

中国版本图书馆 CIP 数据核字（2018）第 107539 号

责任编辑：庞从容　唐仲江　　**责任校对**：谷　洋

文字编辑：薛迎春　　**责任印制**：卢运霞

侦查中电子数据取证

ZHENCHAZHONGDIANZISHUJUQUZHENG

李双其　林　伟　著

出版发行：知识产权出版社有限责任公司　网　　址：http://www.ipph.cn

社　　址：北京市海淀区气象路 50 号院　邮　　编：100081

责编电话：010-82000860 转 8726　责编邮箱：pangcongrong@163.com

发行电话：010-82000860 转 8101/8102　发行传真：010-82000893/82005070/82000270

印　　刷：北京嘉恒彩色印刷有限责任公司　经　　销：各大网上书店、新华书店及相关专业书店

开　　本：710mm×1000mm　1/16　印　　张：19.5

版　　次：2018 年 6 月第 1 版　印　　次：2018 年 6 月第 1 次印刷

字　　数：327 千字　定　　价：55.00 元

ISBN 978-7-5130-5580-2

厦门市美亚柏科信息股份有限公司
福建中锐电子科技有限公司 资助出版

前　言

本书将电子数据取证限定在侦查中。也就是说，本书仅论及刑事侦查活动中的电子数据取证，排除了民事、行政及其他诉讼活动中的电子数据取证。

本书使用“电子数据”一词，不用电子证据、数字证据、电子物证等词汇，与现行《刑事诉讼法》保持一致。

本书采用“电子数据取证”一词，不用电子证据取证、数字证据取证、电子证据检查、电子数据收集、电子数据采集、电子物证勘验、计算机犯罪现场勘验等词。我们认为，关于“电子数据取证”，不同时期采用的名称不一样。依据《刑事诉讼法》《民事诉讼法》《行政诉讼法》对于“电子数据”的界定，我们认为现统一称“电子数据取证”较合适。

“在侦查过程中，电子数据取证的目标是‘电子数据’，使用的方法是获取和证实。电子数据取证是一个动态的过程。对于电子数据取证来说，取和证是一个闭环的过程。”[1]通常把电子数据界定为案件发生过程中形成的，以数字化形式存储、处理、传输的，能够证明案件事实的数据。通常把电子数据取证理解为采用技术手段，获取、分析、固定电子数据作为认定事实的科学过程。

取证是一个动态复杂的过程，主要包含两方面工作：一是获取，一是证实。获取表现为寻找发现、固定记录、收集提取、保全归档等具体的动作，证实表现为审查、分析、判断、出示等具体的行为。

以数字化形式存储、处理、传输的，能够证明案件事实的数据种类繁多，十分复杂；取证也是一个复合性词汇，两者叠加，可见电子数据取证是一项十分繁杂的活动。

在我国，关于电子数据取证，自计算机犯罪、网络犯罪出现后，便有人开始对其进行研究。特别是2012年修改的《刑事诉讼法》实施后，

---

〔1〕 刘浩阳编著．网络犯罪侦查．清华大学出版社，2016：350.

研究电子数据取证的人逐渐增多，同时有不少关于“电子数据取证”的著作面世。但相关著作的研究视角大都立足于所谓的“专业技术人士”，而非立足于侦查人员。我们认为，当信息技术与人们的工作生活相融得十分密切之时，电子数据已成为了一种无处不在的“痕迹”。开展侦查活动中，无论面对的是怎样的案件，几乎都要面对、处理电子数据。就是说，电子数据取证不再仅仅是面对计算机犯罪、网络犯罪时要做的事。处理电子数据应成为侦查人员的常态化工作，而非特定人的特殊工作。合法科学地处理电子数据应成为侦查人员的一种基本能力。基于这样的思路，本书立足于侦查，以侦查人员如何合法科学地处理电子数据为研究视角，把侦查人员如何合法科学地处理电子数据取证作为论述的重点。同时，鉴于现有大多数侦查人员的知识结构，本书尽量将复杂的技术问题简单化，尽量将复杂的技术问题进行具有可操作性的论述，让侦查人员在学习中能够尽快明确电子数据取证相关知识，尽快初步掌握电子数据取证技能。可以说，这既是研究本课题的价值，也是撰写本书的基本意图。

作案人在作案过程中会留下电子数据，这不以作案人的意志为转移，电子数据客观存在。在将电子数据作为一种证据写入《刑事诉讼法》之前，侦查人员在取证时并不太注重电子数据的收集提取，收集提取电子数据成了一件可有可无之事。当有能力时取之，无能力时不取。那时，电子数据取证主要是针对计算机犯罪、网络犯罪案件。在其他案件的侦查中，电子数据主要被用于发现侦查线索，还谈不上当作证据使用。随着信息技术的广泛运用，作案人在作案过程中留下电子数据变得十分普遍，因此，电子数据作为证据之一被写入《刑事诉讼法》，至此电子数据的收集提取、审查判断与鉴定运用便成为了一个不得不正视的问题。

但是，在侦查实践中，侦查人员并不能够很好地解决电子数据的收集提取、审查判断等问题。电子数据类证据包括哪些？电子数据类证据的法律地位如何？电子数据具有怎样的证明力？侦查过程中，该由具体的哪个部门去收集提取电子数据？收集提取电子数据需要用到哪些工具和技术？应采用怎样的方法对电子数据进行收集提取？该如何对电子数据类证据进行审查判断？……许多基本问题摆在侦查人员的面前，电子数据被写入《刑事诉讼法》后，它的收集提取和审查判断等就成了侦查

工作中的热点和难点。在本课题组成员调研时，各地公安机关侦查部门均有反映：如何应对电子数据是目前侦查工作中最让人头疼的事情之一。因此，对电子数据的收集提取和审查判断等基本问题进行研究是很有实用价值的。

近年来，有不少关于电子数据取证的著作面世，通观已有的研究成果，成果零散性特征较为突出，尤其是缺乏从侦查角度对电子数据类证据的收集提取、审查判断的系统研究。现有研究成果缺乏与侦查工作的密切联系，不能很好地帮助侦查办案人员有效地解决电子数据取证问题。关涉电子数据收集提取和审查判断的若干基本问题尚未厘清，侦查办案人员在面对电子数据时尚未找到可靠的理论依据。同时，现有的侦查学教科书里关于电子数据的收集提取和审查判断仍然是空白点。从这个角度看，对侦查中电子数据取证问题进行研究也是很有价值的。

从世界范围看，有些学者致力于将计算机技术引入电子取证中，例如云存储、数据挖掘、数据文件完整性校验技术等。他们利用先进的电子取证设备进行取证，保证数据的合法性，然后用于法律诉讼。还有些学者专注于电子取证调查过程的标准化和规范化研究，提出跨国间电子数据采集标准的统一，以效力于跨国犯罪案件。国外学者一致认为，区别于传统的调查取证，电子取证对于侦查人员的技术要求更高，这就迫切需要提高相关人员的专业性，并形成规范的证据程序。有学者呼吁，应该尽快利用丰富的电子数据资源，建立结构完整、程序齐全的电子取证体系，以提高破案效率。发达国家在电子取证方面走在了世界的前列。美国及欧洲一些国家均制定了“电子证据规则”。不少学者也致力于电子证据的研究，并有不少成果面世。国内一些学者已将美国及欧洲的电子取证研究成果翻译到国内。国外的研究成果是值得借鉴的，与国内的研究成果相比，其更注重从侦查角度出发对电子取证问题进行研究，但结合得仍然不够。同时，由于法治环境不同，国外的研究成果只能作为参考。

尽管国内外有关人士对电子数据取证的研究取得了一定的成就，但由于电子数据取证问题极其复杂，可以说，目前对这一问题的研究仍然处于初级阶段。大量的基础问题并未得到很好的研究解决，主要表现在：若干基本概念并未得以明确；取证环节依据不足；认证规则并未得以确

认；取证标准并未得以统一；电子数据类证据的法律地位并未达成共识；取证工具和技术并未得到有效的权威性认证；电子数据的收集提取并没有具体的依据可循；如何对电子数据进行审查判断并没有有力的理论支持；在面对不同环境中的具体电子数据时，侦查人员常常无从下手。实践中，取证者仍停留于初学者状态。专业的取证者沉浸于技术。办案的侦查人员还只能被动、盲目地应对电子数据。技术与法律、侦查的结合还很不理想、很不到位。

当上述一系列基础问题尚未得以很好回应和解决之时，由于信息技术的升级及犯罪分子的加以利用，犯罪也出现了升级。由于升级版犯罪的出现，新型虚拟空间变得愈发多样，出现了以前从未出现过的虚拟空间，出现了新型的电子数据。这些存在于新型虚拟空间里的新型电子数据，处理时将更加没有依据，处理起来的难度也将大大提高。因此，在研究与电子数据取证有关的基础问题时，还得回应犯罪升级，回应因犯罪升级而引发的犯罪空间及电子痕迹的变化所带来的种种问题。

主要法律法规、司法解释全称与简称对照

《中华人民共和国刑事诉讼法》，简称《刑事诉讼法》

《中华人民共和国刑法》，简称《刑法》

《中华人民共和国电子签名法》，简称《电子签名法》

《中华人民共和国网络安全法》，简称《网络安全法》

《最高人民法院　最高人民检察院　公安部关于办理刑事案件收集提取和审查判断电子数据若干问题的规定》，简称《收集提取和审查判断电子数据问题规定》

《最高人民法院关于民事诉讼证据的若干规定》，简称《关于民事诉讼证据的若干规定》

《最高人民法院关于适用〈中华人民共和国刑事诉讼法〉的解释》，简称《刑事诉讼法解释》

《全国人民代表大会常务委员会关于司法鉴定管理问题的决定》，简称《关于司法鉴定管理问题的决定》

目录

第一章　电子数据及取证概述

一、电子数据的含义

提到“电子数据”一词时，不得不提到“电子证据”一词。在2012年修订的《刑事诉讼法》实施之前，大多数人都用“电子证据”一词——不管是研究者，还是实务部门实践者。在与电子数据取证相关的著作、教科书、论文里，“电子证据”一词十分多见，而“电子数据”一词十分少见。但在2012年修改的《刑事诉讼法》实施之后，情况发生了变化——“电子数据”一词渐渐多用，而“电子证据”一词渐渐少用。现在的情景是：电子证据与电子数据共用。有的人甚至把两个词混用而不加区分。

我们主张与现行《刑事诉讼法》保持一致，用“电子数据”一词，而不用别的词汇或术语。

当然，由于历史原因，当在理解“电子数据”的含义时，先不得不理解一下“电子证据”的含义。

“电子证据这一术语的出现并不久远，20世纪80年代在西方国家的论著和立法中方才显现，20世纪90年代末输入我国。在西方国家的证据理论和实践中，指代电子证据的表述有很多，诸如‘electronic evidence’‘digital evidence’‘computer evidence’‘computer-produced evidence’‘computer-created evidence’‘computer-based evidence’‘computer-related evidence’‘computer output’‘computer-stored evidence’‘evidence from computer record’等。在我国的证据法理论和实践的语境中，电子证据的指称方式亦有多种，譬如‘电子数据’‘电子证据’‘计算机证据’‘数据证据’‘网络证据’‘数据电文证据’‘电子数据证据’等。”[1]在我国的侦查学界，有些人还把电子数据称为电子物证。

---

[1] 刘显鹏．电子证据认证规则研究——以三大诉讼法修改为背景．中国社会科学出版社，2016：2.

“电子证据与传统证据最大的区别在于，其将人们所要表达的意思转化为信号，并通过特定的数字技术呈现在一定的电子设备或电磁介质之上，可以说基本上是‘了无痕迹’，充其量也只是一些打印或保存在电子设备或介质上的数据，而一经从储存系统中删除，便基本上完全‘无影无踪’；而打印或保存在电子设备或介质上的数据因易于伪造或删改而使人们对其收集、保存和运用顾虑重重，故电子证据保全的要求较之普通证据要更为严格。”[1]

通常，对电子证据我们可以作这样的理解：电子证据是经由一定的电子设备和技术生成的、以数字信息化的编码形式出现的、用以存储并记载相关信息且可反映特定案情的所有类型的数字化的记录和信息。电子证据通常包含以下三项要素：一是电子证据以电子形式表现出来；二是电子证据必须借用特定的电子设备方能展示；三是电子证据是作为证据使用的材料。

有人将电子证据等同于电子数据，认为电子证据或电子数据是指以电子形式生成，以数字化形式存在于磁盘、光盘、计算机等载体，用以证明案件事实的电磁记录物。[2]

相关人员在论著中对电子数据是这样界定的：“电子数据就是信息数字化过程中形成的以数字形式存在的能够证明案件事实情况的数据。”[3]

“电子数据”一词与电子证据、数字证据、电子证据、网络证据等术语没有质的不同。它们只是不同时期、不同行业或不同人群对所谓的电子数据类证据的不同称呼而已。称谓的杂乱，“非但没能使电子数据易于理解，反而加大了理解的复杂度，使得取证领域拘泥于概念的论战，陷入单纯的学派之争，这既不利于法律的实施，也不利于这一领域的发展。”[4]

在我国，2012 年修改的《刑事诉讼法》实施之后，尤其是《收集提取和审查判断电子数据问题规定》发布后，关于电子数据称谓的统一已经不再是难题，对电子数据概念的界定也不再是需要多方辨析的问题了。2016 年 9 月 20 日，最高人民法院、最高人民检察院、公安部为规范电子数据的收集提取和审查判断，提高刑事案件办理质量，根据《刑事诉讼法》等有关法律规定，结合司法实际，制定并发布了《收集提取和审查判断电子数据问题规

---

〔1〕 刘显鹏．电子证据认证规则研究——以三大诉讼法修改为背景．中国社会科学出版社，2016：202.

〔2〕 汪振林等编．电子证据学．中国政法大学出版社，2016：7.

〔3〕 刘浩阳编著．网络犯罪侦查．清华大学出版社，2016：350.

〔4〕 刘浩阳，李锦，刘晓宇主编．电子数据取证．清华大学出版社，2015：3.

定》，在该规定的第一条对电子数据进行了明确的界定：电子数据是案件发生过程中形成的，以数字化形式存储、处理、传输的，能够证明案件事实的数据。

可以说，这是迄今为止最为权威的界定。本书在论述电子数据时，对电子数据的理解以《收集提取和审查判断电子数据问题规定》的规定为依据。

当然，按照《收集提取和审查判断电子数据问题规定》对电子数据的界定，理解起来仍然会有歧义。这里的问题是：一是电子数据是否一定是“案件发生过程中形成”，值得商榷。比如说，某犯罪嫌疑人注册了一个 QQ 电子邮箱，一般来说，涉案的 QQ 电子邮件内容可能是案件发生过程中形成的。但是 QQ 电子邮箱的用户注册信息，显然是案件发生之前形成的。不能否认的是，QQ 电子邮箱的用户注册信息对于案件事实及嫌疑人的认定具有重要的证明价值，属于能够证明案件事实的电子数据。当然，有人还会这样去解释，注册 QQ 电子邮箱是犯罪的组成部分。注册 QQ 电子邮箱归于犯罪的预备。如果这样去理解，QQ 电子邮箱的注册行为也就属于案件发生过程中形成的了。但是，在现实中的确会遇到某一 QQ 电子邮箱是某人在很早以前注册的，很久以后这人才利用这个电子邮箱实施犯罪。此时，该 QQ 电子邮箱是不是“案件发生过程中形成的”就难说了。二是电子数据是否一定以“数字化”的形式存储、处理和传输，值得商榷。“数字化”是一个引自信息技术领域的概念。随着信息技术的发展，绝大多数的信息目前都已经以数字信息的形式来表达。然而，毕竟还存在不少以模拟信号形式表达的数据，比如以磁带、胶片等方式存储的声音、图像信息。这些以模拟信号形式存储的数据信息，是否还是电子数据呢？对这一问题的理解一定会存在争议。当然，如果简单把非数字化的信息资源不归入电子数据，那也就好理解了。用“数字化”形式来归纳电子数据的特点倒是人们所接受的。三是电子数据是“……的数据”，值得商榷。根据逻辑学下定义的范式，对电子数据进行定义需要引用一个属概念。这里采用了“数据”作为“电子数据”的属概念，是否合适也值得讨论。

当然，商榷归商榷，本书还是以《收集提取和审查判断电子数据问题规定》对电子数据的界定来理解电子数据。根据该规定的界定，可以这样理解：只要是在案件发生过程中形成的，以数字化形式存储、处理、传输的，能够证明案件事实的数据都可以称为电子数据。可见，电子数据种类何其多，范围何其广。

在侦查实践中，当面对具体的数据时，究竟能不能将其认定为电子数据仍然不好把握。把实践中认定电子数据的难题一一排开并对它们进行比较，我们会发现，在许许多多的难题中，最大的难题是对2012年修改的《刑事诉讼法》规定的第八种法定证据形式“视听资料与电子数据”的辨别。

2012年修改的《刑事诉讼法》将视听资料与电子数据列为第八种法定证据形式，但是该法及相关司法解释却并没有对视听资料与电子数据作出明确的界定，因此导致这两种证据在理论和实务中交叉混淆。根据文理解释，视听资料是指录音、录像等通过视觉和听觉可以直观感受的证据资料。而电子数据是指以数字化形式存储、处理、传输的，能够证明案件事实的数据。在此存在两种定义标准：一个是从对证据感知的角度下定义，一个是从证据保存的方式下定义。两个并列的证据完全没有在同一逻辑层面上。这就不可避免地出现了重叠交叉。比如，监控视频记录下来的某作案人的犯罪视频资料，究竟是属于视听资料还是电子数据？根据视听资料和电子数据的文理解释，这段视频同时符合两个定义的要求，让人难以适从。显然，这种随意性的并列不利于取证、举证、质证和认证等具体实务。尽管《收集提取和审查判断电子数据问题规定》对电子数据类证据进行了具体的分类和列举，但由于上位法的模糊，仍然导致实践中对电子数据类证据难以区分。[1]

不少学者建议，在《刑事诉讼法》规定的第八种法定证据里，将视听资料去除，保留电子数据证据。对此，我们持赞同观点。理由是：在信息技术广泛应用的时代，“电子数据”一词足以囊括视听资料对应的证据范围；以电子数据的取证、质证、认证程序来收集提取视听资料，足以确保其可采性；去除视听资料可以化繁就简，排除干扰混淆。另外，电子数据的命名符合世界潮流，视听资料的证据命名方式在外国证据法中并不多见。

二、电子数据的分类

电子数据与其他证据形式不同，不仅其来源多种多样，存储介质种类繁多，生成机理差异较大，而且其作用也各有不同，因此对电子数据进行分类是一个复杂的问题。电子数据是一种数字化的记录和信息，是0与1进位记

〔1〕 刘思雨．刑事诉讼中电子数据面临的困境及其对策．江苏警官学院学报，2015（4）：117.